What is claimed is:

1. A method for using an encrypted file in e-commerce on the internet which comprises the steps of:

creating said file, with said file having a first part and a second part;

encrypting said first part of said file with a first private key, wherein said first part of said file includes a second private key; and

encrypting said second part of said file with said second private key.

2. A method as recited in claim 1 further comprising the steps of:

decrypting said first part of said file with said first private key in response to a commercial transaction between a seller and a buyer;

retrieving said second private key from said first part; and

decrypting said second part of said file with said second key.

3. A method as recited in claim 2 further comprising the steps of:

presenting said file on the Internet, wherein said presenting step is accomplished by the seller;

selecting said file from the Internet, wherein said selecting step is accomplished by the buyer; and

sending said first part of said file to a transaction agent for decrypting said second part of said file.

4. A method as recited in claim 3 wherein said commercial transaction is accomplished using the steps of:

debiting a buyer's account for a predetermined amount by said transaction agent in response to said sending step; and

crediting a seller's account with said predetermined amount by said transaction agent in response to said debiting step.

5. A method as recited in claim 2 wherein decrypting said first part requires a first operation and decrypting said second part requires a second operation.

6. A method as recited in claim 5 wherein said first operation is the same as said second operation.

7. A method as recited in claim 1 wherein said first private key and said second private key are provided by the seller.

8. A method as recited in claim 1 wherein said step of decrypting said first part is accomplished by said transaction agent.

9. A method as recited in claim 1 wherein said step of decrypting said second part is accomplished by the buyer.

10. A method as recited in claim 1 wherein said second part is a content, and further wherein said content includes work selected from a group consisting of books, documents, pamphlets, movies, songs, games, pictures and software.

11. A system for conducting a secure transaction in e-commerce over the Internet which comprises:

a means for use by a seller for creating an internet file, said file having a first part containing administrative information about said file and a second part containing a content including transactional subject matter;

a first private key for encrypting said first part;

a second private key for encrypting said second part; and

a means for releasing said second key for use in decrypting said second part to reveal said content to a buyer.

12. A system as recited in claim 11 wherein said second private key is provided by the seller.

13. A system as recited in claim 11 wherein said first key is provided by a transaction agent.

14. A system as recited in claim 11 wherein said content of said file has a value established by a seller and said system further comprises:

a buyer's account maintained by a transaction agent for the buyer;

a seller's account maintained by the transaction agent for the seller; and

a means for transferring funds of said value from the buyer's account to the seller's account when said second part of said file is revealed.

15. A system as recited in claim 11 wherein said file further contains a clear-text header, with said header including advertising material and commercial material about said file, and further wherein said content of said second part includes work selected from a group consisting of books, documents, pamphlets, movies, songs, games, pictures and software.

16. A method for conducting encrypted commercial transactions between a buyer and a seller, wherein said method involves a transaction agent and comprises the steps of:

presenting a file, said file being created by the seller and containing at least an overhead and a content, with said overhead being encrypted with a first private key and said content being encrypted with a second private key; and

decrypting said content of said file by employing said second private key to reveal said content of said file for use by the buyer in response to a commercial transaction between the buyer and the seller.

17. A method as recited in claim 16 wherein said presenting step is accomplished on an Internet.

18. A method as recited in claim 16 wherein said decrypting step is accomplished by the transaction agent.

19. A method as recited in claim 16 wherein said decrypting step is accomplished by the buyer.

20. A method as recited in claim 16 wherein said first private key is known to only the transaction agent and the seller for encrypting/decrypting said content of said file.

## ABSTRACT

A system and method for transferring an encrypted file over the Internet involves a seller, a buyer, and a transaction agent. The file has a first part (administrative information) and a second part (subject-matter content) that are respectively encrypted with first and second encryption/decryption non-public keys. In operation, the appropriate key is released by the seller or the transaction agent for respective use by either the transaction agent or the buyer, to decrypt and reveal the second part of the file to the buyer.

PATENT: 11298.4.1